



保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

網路釣魚網址的填充、堆疊與使用者資訊濫用手法

2026 年 9 月 1 日發布

 **點擊此處可獲取--最完整的賽門鐵克解決方案資訊**

路釣魚攻擊愈來愈常從網址下手。附件並未絕跡，但攻擊者在連結本身投入了更多工程心力——連結比二進位檔案更省成本、更容易變異，測試成本更是低得多。

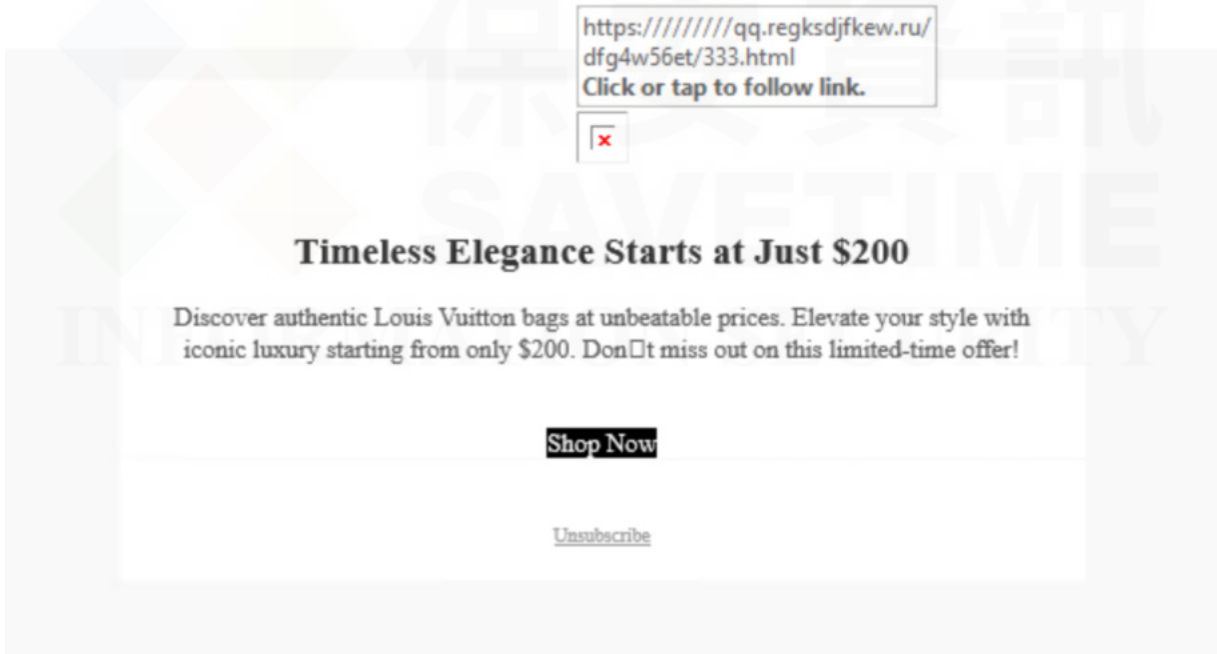
以下是我們最常觀察到的三種手法（過去 10 個月累計阻擋超過 1,600 萬次），以及可有效攔阻這些手法的防護措施。文中所有入侵指標均已淨化並去武器化（defanged）。

多餘分隔符號填充

- `hxxps://example[.]com//////////login.php`
- `hxxps://[legit-looking-domain]////////[malicious-path]`

不過就是多了幾道斜線，別無其他。之所以有效，是因為瀏覽器在剖析特殊協定（special scheme）的授權區段（authority）時，會略過任意長度的連續斜線，而伺服器端也會寬容處理其餘部分——nginx 預設會合併重複斜線，多數框架也是依正規化後的路徑進行路由。這些填充，受害者根本看不出來。

攻擊者的收益在於：變體可無限產生，邊際成本為零；無須註冊任何新資源，就能重複利用已遭識破的基礎架構；而且這是可附加於任何攻擊活動的投遞階段轉換手法。它與釣魚套件無關，這正是其價值的絕大部分所在。



品牌關鍵字子網域堆疊

- `hxxps://login-microsoftonline-com[.]security-check[.]xyz////////oauth////authorize`

這是在子網域而非可註冊網域中進行的組合式搶註（combosquatting）。login-microsoftonline-com 是攻擊者免費建立的標籤；security-check[.]xyz 才是 eTLD+1，也是他們唯一需要購買的部分。只需一次註冊，即可建立無限多個標籤，而且不會像對主要網域進行拼字搶註（typosquatting）那樣，引來網域註冊商的標記。

它利用的是使用者被灌輸而養成的錯誤習慣：只找品牌字串，而不是由右至左解讀 DNS 授權結構。在行動裝置上，網址列會從右側截斷，使用者能看到的往往只剩該標籤。

回報時有一點需要注意：/oauth/authorize 路徑只是幌子。模仿 OAuth 端點屬於偽裝，並不能證明這是同意授權（consent-grant）攻擊——真正的同意授權釣魚，會指向合法的身分提供者，並帶有攻擊者掌控的 client_id。

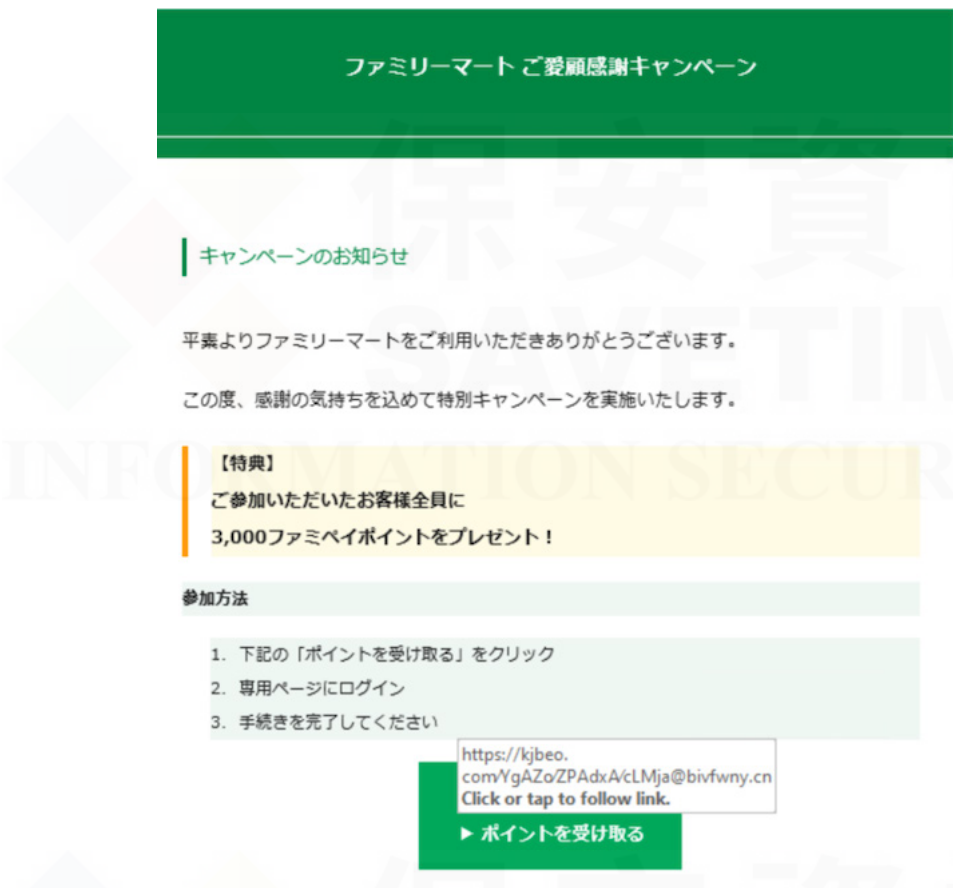
同形異義分隔符號與使用者資訊濫用

- `hxxps://base_domain / YgAZo / ZPAdxA / cLMja@destination_domain[.]cn`

這是兩種手法疊加，且必須搭配才能奏效。/ 為 U+2215（DIVISION SLASH，除法斜線），外觀與 ASCII 的 / 幾乎無法分辨，卻是不同的編碼位置，因此只認 ASCII / 的詞元剖析器（tokenizer）永遠找不到授權區段的結尾。授權區段中未經跳脫的 @ 之前的所有內容，都屬於使用者資訊（userinfo），因此瀏覽器會捨棄 base_domain / YgAZo / ZPAdxA / cLMja，並連線至 destination_domain[.]cn。

這些假斜線讓使用者資訊區段得以拉長，長到足以容納一個以假亂真的主機名稱與看似合理的路徑。若改用真正的斜線，授權區段會在第一個斜線處結束，@ 只會無害地落在路徑中，偽裝隨即瓦解。這種相依關係同時也是偵測契機——兩者總是同時出現。

另有一項但書值得注意：瀏覽器會從子資源請求中移除內嵌的認證資訊，而且導覽完成後，網址列會顯示真正的主機。因此，欺騙得逞的時間窗口在於點擊之前，以及行動裝置上——游標停留時的連結預覽、郵件用戶端中的連結文字、被截斷的網址列。這個窗口比五年前更窄，但仍是關鍵所在，因為點擊就是得手的轉換事件。隨機產生的路徑權杖（token）有雙重作用：針對每位受害者進行追蹤，並確保沒有任何兩個投遞出去的網址在位元組上完全相同。



賽門鐵克防護

- 憑證竊取不會投放任何檔案，因此這類威脅主要出現在網頁與電子郵件層——唯有攻擊活動帶有惡意酬載分支時，端點的檔案防護才會派上用場。賽門鐵克在電子郵件與網頁攻擊管道提供多層防禦，以因應這些規避手法。

網頁情資與攔道

- 所有啟用 WebPulse 的攔道，都會持續分析、分類並阻擋惡意基礎架構，包括惡意網域與 IP 位址。

電子郵件安全與虛擬化

- 賽門鐵克的電子郵件安全解決方案，針對網頁型連結威脅提供端到端防護，並運用賽門鐵克郵件威脅隔離（Email Threat Isolation，簡稱：ETI），在隔離的虛擬瀏覽器環境中化解惡意網址。
- 透過賽門鐵克全球情資網路（Global Intelligence Network，簡稱：GIN），過去 10 個月已成功阻擋約 1,600 萬封與這些攻擊活動相關的垃圾郵件。

端點

- 賽門鐵克端點安全完整版（SES Complete）的入侵防護系統（IPS）技術取材自 GIN，將來自賽門鐵克整體客戶群的威脅情資帶入端點防護。

行動裝置

- Symantec Endpoint Protection Mobile 能分析簡訊（SMS）中所含的連結，透過比對文字訊息中的網址與賽門鐵克 WebPulse（屬於 GIN 的一部分）中的威脅情資，保護使用者免受簡訊釣魚攻擊，並在連結可疑時向使用者示警。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-padding-stuffing-and-userinfo-abuse-in-phishing-urls
本文文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以Symantec原廠公告為準，請知悉。



關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉康創辦的企業軟體公司，組合國際電腦 (CA Technologies) 以及雲端運算及「硬體虛擬化」的領導廠商--VMware，也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署 (CISA) 宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC (Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。



關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。
保安資訊連絡電話：0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家

 We Keep IT Safe, Secure & Save you Time, Cost 

服務電話：0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>